

EXTENSIONS OF GROUP SCHEMES OF μ -TYPE BY A CONSTANT GROUP SCHEME

HENDRIK VERHOEK

ABSTRACT. For a number field K , a finite set of primes S not containing a fixed prime p , we explain when extensions of group schemes of μ_p by $\mathbf{Z}/p\mathbf{Z}$ split over the ring of S -integers O_S of K .

CONTENTS

1. Introduction	1
2. Extensions of modules	1
3. Extensions of group schemes	3
4. Example calculations	5
References	7

1. INTRODUCTION

Let p be a rational prime and K a number field. Let S be a finite set of primes in K that does not contain primes above p . Let π be a prime ideal above p in O_S and let $\widehat{O_S}$ be the completion of O_S at π . Denote by $\text{Ext}_{O_S}^1(\mu_p, \mathbf{Z}/p\mathbf{Z})$ the group of equivalence classes of extensions of μ_p by the constant group scheme $\mathbf{Z}/p\mathbf{Z}$ in the category of finite flat commutative group schemes over O_S . Our main goal is to calculate the group $\text{Ext}_{O_S}^1(\mu_p, \mathbf{Z}/p\mathbf{Z})$:

Theorem 1.1. *Suppose p does not split in K/\mathbf{Q} . Let $\widehat{L} = \widehat{O_S}[\zeta_p/p]$ and $\omega : \text{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \rightarrow \mathbf{F}_p^*$ be the cyclotomic character at p . Suppose that the ω^2 -eigenspace of the p -torsion of the class group of $O_S[\zeta_p/p]$ is trivial. Then*

$$\text{Ext}_{O_S}^1(\mu_p, \mathbf{Z}/p\mathbf{Z}) \simeq_{\mathbf{F}_p} \ker \left((O_S[\zeta_p/p]^* / (O_S[\zeta_p/p]^*)^p)_{\omega^2} \longrightarrow (\widehat{L}^* / (\widehat{L}^*)^p)_{\omega^2} \right).$$

Finite flat commutative group schemes of p -power order over a base where p is invertible, are étale group schemes and therefore just Galois modules. Therefore we will consider in Section 2 extensions of modules with a group action. In Section 3 we move on to extensions of the finite flat group schemes $\mathbf{Z}/p\mathbf{Z}$ by μ_p that are killed by p and prove Theorem 1.1. Finally, we calculate for various K and S the group $\text{Ext}_{O_S}^1(\mu_p, \mathbf{Z}/p\mathbf{Z})$ using Theorem 1.1.

2. EXTENSIONS OF MODULES

Let R be a commutative unitary ring such that $p \cdot R = 0$ and let G be a group. When we say R -module, we mean a left R -module. We will consider extensions of R -modules with an action of G , as a preparation for the next section, where we will discuss extensions of finite flat group schemes. We will use the following theorem of Grothendieck:

Theorem 2.1. *Let C_1, C_2 and C_3 be abelian categories, such that C_1 and C_2 have enough injectives. Let $F_1 : C_1 \rightarrow C_2$ be a left exact functor that maps injective objects in C_1 to acyclic objects in C_2 and let $F_2 : C_2 \rightarrow C_3$ be a left exact functor. Then there is an exact sequence of low degree terms:*

$$0 \longrightarrow (R^1 F_2)(F_1(A)) \longrightarrow (R^1(F_2 F_1))(A) \longrightarrow \\ F_2((R^1 F_1)(A)) \longrightarrow (R^2 F_2)(F_1(A)) \longrightarrow (R^2(F_2 F_1))(A)$$

Proof. See [Wei94, Theorem 5.8.3, p. 151]. □

Let A and B be two $R[G]$ -modules such that G acts trivially on B and such that H acts trivially on A . Let $\chi : G \rightarrow (\mathbf{Z}/p\mathbf{Z})^*$ and suppose that H is contained in $\ker(\chi)$. Denote by $B(\chi)$ the G -module that has underlying group structure the one of B and where the G -action is given by $\sigma b := \chi(\sigma)b$ for all $\sigma \in G$ and all $b \in B$. We let G act on $\text{Hom}_H(B, A)$ through the action of G on A . Denote by $\text{Hom}_H(B, A)_\chi$ the subgroup of $\text{Hom}_H(B, A)$ on which $\Gamma = G/H$ acts through χ .

Lemma 2.2. *We have the following isomorphisms of groups:*

$$\text{Hom}_G(B(\chi), A) \simeq \text{Hom}_H(B, A)_\chi.$$

Proof. Let $\psi : B \rightarrow B(\chi)$ be an H -linear isomorphism and let $\phi : \text{Hom}_G(B(\chi), A) \rightarrow \text{Hom}_H(B, A)_\chi$ such that $f \mapsto f \circ \psi$. The morphism $f \circ \psi$ is indeed an element in $\text{Hom}_H(B, A)_\chi$ because for all b in B and σ in G the following equalities hold:

$$\begin{aligned} (\sigma(f \circ \psi))(b) &= \sigma((f \circ \psi)(b)) \\ &= f(\sigma(\psi(b))) = f(\chi(\sigma)\psi(b)) \\ &= \chi(\sigma)f(\psi(b)). \end{aligned}$$

Note that the second equality follows because f is G -linear. Next we prove that the inverse morphism of ϕ is just precomposing with ψ^{-1} . For $g \in \text{Hom}_H(B, A)_\chi$ we have $g \circ \psi^{-1} \in \text{Hom}_G(B(\chi), A)$, because for all b in $B(\chi)$ and all σ in G :

$$\begin{aligned} (\sigma(g \circ \psi^{-1}))(b) &= \chi(\sigma)((g \circ \psi^{-1})(b)) \\ &= (g \circ \psi^{-1})(\chi(\sigma)b) \\ &= (g \circ \psi^{-1})(\sigma \cdot b). \end{aligned}$$

□

Proposition 2.3. *Let A and B be two $R[G]$ -modules such that G acts trivial on B and such that H acts trivial on A . Then*

$$\text{Ext}_H^1(B, A)_\chi \simeq \text{Ext}_G^1(B(\chi), A)$$

as R -modules.

Proof. We consider the following two functors: The left exact functor $F_1(\cdot) = \text{Hom}_H(\cdot, A)$ from $R[G]$ -modules to $R[\Gamma]$ -modules and the exact functor F_2 “taking χ -eigenspaces” from the category of $R[\Gamma]$ -modules to $R[\Gamma]$ -modules. With these two functors F_1 and F_2 , we apply Theorem 2.1. Since F_2 is exact, the functors F_1 and F_2 give rise to the exact sequence

$$\begin{aligned} 0 \longrightarrow (R^1 F_2)(\text{Hom}_H(B, A)) &\longrightarrow R^1(F_2 F_1)(B) \\ &\longrightarrow \text{Ext}_H^1(B, A)_\chi \longrightarrow (R^2 F_2)(\text{Hom}_H(B, A)) \longrightarrow \dots \end{aligned}$$

Since F_2 is exact, the $R[\Gamma]$ -modules $R^1(F_2F_1)(B)$ and $\text{Ext}_H^1(B, A)_\chi$ are isomorphic. But $(F_2F_1)(B)$ is isomorphic to $\text{Hom}_G(B(\chi), A)$ by Lemma 2.2.

Define the functor T_1 "twisting with χ " from the category of $R[G]$ -modules to itself, the functor $T_2(\cdot) = \text{Hom}_G(\cdot, A)$ from the category of $R[G]$ -modules to the category of R -modules and the forgetful functor F that forgets the Γ action and goes from the category of $R[\Gamma]$ -modules to the category of R -modules. Then we have a natural isomorphism $FF_2F_1 \simeq T_2T_1$. The functor T_1 sends injective objects to injective objects, which are in particular acyclic objects. Hence, we can apply Theorem 2.1 to get the following exact sequence:

$$0 \longrightarrow (R^1T_2)(B(\chi)) \longrightarrow R^1(T_2T_1)(B) \longrightarrow T_2(R^1T_1(B)) \longrightarrow (R^2T_2)(T_1(B)) \longrightarrow \dots$$

Since T_1 is exact, we obtain that $(R^1T_2)(B(\chi)) = \text{Ext}_G^1(B(\chi), A)$ is isomorphic to $R^1(T_2T_1)(B)$ as R -modules. Putting everything together, we now have isomorphisms of R -modules

$$\text{Ext}_H^1(B, A)_\chi \simeq R^1(F_2F_1)(B) \simeq R^1(T_2T_1)(B) \simeq \text{Ext}_G^1(B(\chi), A),$$

which is what we wanted to show. \square

When we take χ to be the trivial character in Proposition 2.3, we obtain the Γ -invariant extensions, which are as expected just extensions of $R[G]$ -modules. We conclude by remarking that for two $R[G]$ -modules A, B and for a character χ of G , the R -module $\text{Ext}_G^1(A, B)$ is isomorphic to the R -module $\text{Ext}_G^1(A(\chi), B(\chi))$. Here $A(\chi)$ (resp. $B(\chi)$) is the twist of A (resp. B) by χ .

3. EXTENSIONS OF GROUP SCHEMES

Recall that π denotes the prime ideal above p in the ring of S -integers O_S of the number field K . In this section, the ring R will be either the ring of S -integers O_S , the number field K , the completion of O_S with respect to π or the fraction field of such a completion of O_S . Since p does not split in K/\mathbf{Q} , in each case we can talk about the fraction field of R , which we denote by F . Furthermore, let $L = F(\zeta_p)$ and $\Gamma = \text{Gal}(L/F)$.

First we state some facts from [KM85, Section 8.7-8.10]. Let r be a unit in R . Consider the finite flat commutative group scheme

$$T(r) = \text{Spec}\left(\prod_{i=0}^{p-1} R[X_i]/(X_i^p - r^i)\right) = \coprod_{i=0}^{p-1} \text{Spec}(R[X_i]/(X_i^p - r^i))$$

over R . The scheme $T(r)$ is an extension of $\mathbf{Z}/p\mathbf{Z}$ by μ_p . For an R -algebra A , the A -valued points in $T(r)$ are pairs $(a, i/p) \in (A, \mathbf{Q})$ such that $a^p = r^i$ and $0 \leq i \leq p-1$. The group law of $T(r)$ can be described by

$$(a, i/p) \times (b, j/p) = \begin{cases} (ab, (i+j)/p), & i+j < p \\ (ab/r, (i+j-p)/p), & i+j \geq p \end{cases}.$$

The group schemes $T(r^p)$ are split extensions of $\mathbf{Z}/p\mathbf{Z}$ by μ_p and we see that in that case we have:

$$(a, i/p) = (ar^{-i}, 0) \times (r^i, i/p).$$

If r and r' are units in R , then the group schemes $T(r)$ and $T(r')$ are isomorphic if and only if r and r' generate the same subgroup in $R^*/(R^*)^p$.

Lemma 3.1. *The sequence*

$$0 \rightarrow R^*/(R^*)^p \rightarrow \text{Ext}_{R,[p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p) \rightarrow \text{Cl}(R)[p] \rightarrow 0$$

is exact.

Proof. (cf. [Maz77] and [Sch09, Proposition 2.2]). Apply $\text{Hom}(\cdot, \mu_p)$ to the exact sequence of fppf sheaves $0 \rightarrow \mathbf{Z} \rightarrow \mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow 0$ to obtain

$$0 \rightarrow \mu_p(R) \rightarrow \text{Ext}_R^1(\mathbf{Z}/p\mathbf{Z}, \mu_p) \rightarrow \text{Ext}_R^1(\mathbf{Z}, \mu_p) \simeq H_{\text{fppf}}^1(\text{Spec}(R), \mu_p) \rightarrow 0.$$

On the other hand, we apply the global section functor to the Kummer sequence of fppf sheaves

$$0 \longrightarrow \mu_p \longrightarrow \mathbb{G}_m \xrightarrow{[p]} \mathbb{G}_m \longrightarrow 0$$

to obtain

$$0 \rightarrow R^*/(R^*)^p \rightarrow H_{\text{fppf}}^1(\text{Spec}(R), \mu_p) \rightarrow \text{Cl}(R)[p] \rightarrow 0,$$

where $\text{Cl}(R)$ is the class group of R . The lemma follows by [Sch09, Proposition 2.2 i)] that says that $H_{\text{fppf}}^1(\text{Spec}(R), \mu_p) \simeq \text{Ext}_{R,[p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)$. \square

We focus again on the group $\text{Ext}_{O_S}^1(\mu_p, \mathbf{Z}/p\mathbf{Z})$. If R is a completion of O_S at π , the group $\text{Ext}_R^1(\mu_p, \mathbf{Z}/p\mathbf{Z})$ is trivial since μ_p is connected and the connected-étale exact sequence gives a section for such extensions. Therefore, extensions of μ_p by $\mathbf{Z}/p\mathbf{Z}$ are locally split and hence killed by p . Since the completion of O_S at π is flat over O_S , extensions of μ_p by $\mathbf{Z}/p\mathbf{Z}$ over the ring O_S are also killed by p and $\text{Ext}_{O_S}^1(\mu_p, \mathbf{Z}/p\mathbf{Z}) = \text{Ext}_{O_S,[p]}^1(\mu_p, \mathbf{Z}/p\mathbf{Z})$. Let $\omega : \Gamma = \text{Gal}(L/F) \rightarrow \mathbf{F}_p^*$ be the character such that for all $\sigma \in \Gamma$ we have $\sigma(\zeta_p) = \zeta_p^{\omega(\sigma)}$. The scheme μ_p over $R[\zeta_p/p]$ is a constant group scheme and $(\mu_p)_{R[\zeta_p/p]} \simeq_{\mathbf{F}_p} (\mathbf{Z}/p\mathbf{Z})_{R[\zeta_p/p]}$. For integers $0 \leq i, j \leq p-2$ we have the following isomorphisms of \mathbf{F}_p -modules:

$$\text{Ext}_{R[\zeta_p/p]}^1(\mathbf{Z}/p\mathbf{Z}(\omega^i), \mathbf{Z}/p\mathbf{Z}(\omega^j)) \simeq_{\mathbf{F}_p} \text{Ext}_{R[\zeta_p/p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p).$$

Lemma 3.2. $\text{Ext}_{R[1/p],[p]}^1(\mathbf{Z}/p\mathbf{Z}(\omega^i), \mu_p) \simeq_{\mathbf{F}_p} \text{Ext}_{R[\zeta_p/p],[p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)_{\omega^i}$.

Proof. This follows immediately from Proposition 2.3. \square

Corollary 3.3. *If $\zeta_p \notin R$, then $\text{Ext}_{R[\zeta_p/p],[p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p) \simeq_{\mathbf{F}_p} \bigoplus_{i=0}^{p-2} \text{Ext}_{R[1/p],[p]}^1(\mathbf{Z}/p\mathbf{Z}(\omega^i), \mu_p)$.*

Proof. The group $\text{Ext}_{R[\zeta_p/p],[p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ is an $\mathbf{F}_p[\Gamma]$ -module. Hence it can be decomposed as

$$\text{Ext}_{R[\zeta_p/p],[p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p) \simeq_{\mathbf{F}_p[\Gamma]} \bigoplus_i \text{Ext}_{R[\zeta_p/p],[p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)_{\omega_i}.$$

By Lemma 3.2 each summand is isomorphic to $\text{Ext}_{R[1/p],[p]}^1(\mathbf{Z}/p\mathbf{Z}(\omega^i), \mu_p)$ as an \mathbf{F}_p -module. \square

Lemma 3.4 ([Sch03], Corollary 2.4). *Let J' and J'' be two finite flat commutative group schemes over O_S , let p be a prime and let $\widehat{O_S} = (O_S \otimes \mathbf{Z}_p)$. Then the following sequence is exact:*

$$\begin{aligned} 0 \rightarrow \text{Hom}_{O_S}(J'', J') &\rightarrow \text{Hom}_{\widehat{O_S}}(J'', J') \times \text{Hom}_{O_S[1/p]}(J'', J') \rightarrow \text{Hom}_{\widehat{O_S}[1/p]}(J'', J') \\ &\rightarrow \text{Ext}_{O_S}^1(J'', J') \rightarrow \text{Ext}_{\widehat{O_S}}^1(J'', J') \times \text{Ext}_{O_S[1/p]}^1(J'', J') \rightarrow \text{Ext}_{\widehat{O_S}[1/p]}^1(J'', J') \end{aligned}$$

Lemma 3.5. *If p does not split in K/\mathbf{Q} , then $\text{Hom}_{O_S[1/p]}(\mu_p, \mathbf{Z}/p\mathbf{Z}) \simeq \text{Hom}_{\widehat{O_S}[1/p]}(\mu_p, \mathbf{Z}/p\mathbf{Z})$.*

Proof. If $\zeta_p \in K$ then both groups are cyclic of order p . If $\zeta_p \notin K$ then both groups are trivial. \square

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. Consider the exact sequence of $\mathbf{F}_p[\Gamma]$ -modules of Lemma 3.1:

$$0 \rightarrow O_S[\zeta_p/p]^*/(O_S[\zeta_p/p]^*)^p \rightarrow \text{Ext}_{O_S[\zeta_p/p], [p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p) \rightarrow \text{Cl}(O_S[\zeta_p/p])[p] \rightarrow 0.$$

The sequence is still left exact after taking ω^2 -eigenspaces. The condition that the ω^2 -eigenspace of the p -torsion of the class group $O_S[\zeta_p/p]$, denoted by $\text{Cl}(O_S[\zeta_p/p])[p]_{\omega^2}$, is trivial implies that

$$(O_S[\zeta_p/p]^*/(O_S[\zeta_p/p]^*)^p)_{\omega^2} \simeq_{\mathbf{F}_p[\Gamma]} \text{Ext}_{O_S[\zeta_p/p], [p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)_{\omega^2}.$$

Remember that we assume that p does not split in K/\mathbf{Q} , hence $\widehat{O_S}[1/p]$ is a field. We obtain from Lemma 3.4, together with Lemma 3.5, the following exact sequence of \mathbf{F}_p -modules:

$$(1) \quad 0 \rightarrow \text{Ext}_{O_S, [p]}^1(\mu_p, \mathbf{Z}/p\mathbf{Z}) \rightarrow \text{Ext}_{O_S[1/p], [p]}^1(\mu_p, \mathbf{Z}/p\mathbf{Z}) \rightarrow \text{Ext}_{\widehat{O_S}[1/p], [p]}^1(\mu_p, \mathbf{Z}/p\mathbf{Z}).$$

Twisting by the character ω gives the following two isomorphisms:

$$\begin{aligned} \text{Ext}_{O_S[1/p]}^1(\mu_p, \mathbf{Z}/p\mathbf{Z}) &\simeq_{\mathbf{F}_p} \text{Ext}_{O_S[1/p]}^1(\mathbf{Z}/p\mathbf{Z}(\omega^2), \mu_p) \\ \text{Ext}_{\widehat{O_S}[1/p]}^1(\mu_p, \mathbf{Z}/p\mathbf{Z}) &\simeq_{\mathbf{F}_p} \text{Ext}_{\widehat{O_S}[1/p]}^1(\mathbf{Z}/p\mathbf{Z}(\omega^2), \mu_p). \end{aligned}$$

In particular, we have isomorphisms between the p -torsion subgroups of these extension groups. From (1) we obtain

$$0 \rightarrow \text{Ext}_{O_S, [p]}^1(\mu_p, \mathbf{Z}/p\mathbf{Z}) \rightarrow \text{Ext}_{O_S[1/p], [p]}^1(\mathbf{Z}/p\mathbf{Z}(\omega^2), \mu_p) \rightarrow \text{Ext}_{\widehat{O_S}[1/p], [p]}^1(\mathbf{Z}/p\mathbf{Z}(\omega^2), \mu_p).$$

By Lemma 3.2 we obtain

$$0 \longrightarrow \text{Ext}_{O_S}^1(\mu_p, \mathbf{Z}/p\mathbf{Z}) \longrightarrow (O_S[\zeta_p/p]^*/(O_S[\zeta_p/p]^*)^p)_{\omega^2} \longrightarrow (\widehat{L}^*/(\widehat{L}^*)^p)_{\omega^2}.$$

\square

4. EXAMPLE CALCULATIONS

We calculate, using the isomorphism of Theorem 1.1, for specific p and O_S the extension group $\text{Ext}_{O_S}^1(\mu_p, \mathbf{Z}/p\mathbf{Z})$. We will use the following lemma in the computations:

Lemma 4.1. *The group $\mathbf{Q}_2^*/(\mathbf{Q}_2^*)^2$ is generated by 2, 3 and 5. For $p > 2$ the group $\mathbf{Q}_p^*/(\mathbf{Q}_p^*)^p$ is generated by p and $1 + p$.*

Proof. We have the following isomorphism of groups:

$$(2) \quad \mathbf{Q}_p^* \simeq \mu_{p-1} \times p^{\mathbf{Z}} \times (1 + p\mathbf{Z}_p).$$

First we consider the case $p > 2$. Then $(\mathbf{Q}_p^*)^p = \mu_{p-1} \times p^{p\mathbf{Z}} \times (1 + p^2\mathbf{Z}_p)$, where we used Hensel's Lemma to obtain the equality $(1 + p\mathbf{Z}_p)^p = (1 + p^2\mathbf{Z}_p)$. The lemma follows from.

Now suppose that $p = 2$. A unit $x \in \mathbf{Z}_2^*$ is a square if and only if $x \equiv 1 \pmod{8}$. The lemma follows again from the isomorphism (2) and the fact that 3 and 5 are independent mod \mathbf{Q}_2^{*2} : if they were not independent, 15 would be a square in \mathbf{Q}_2 , but $15 \not\equiv 1 \pmod{8}$. \square

The extension group $\text{Ext}_{\mathbf{Z}[\frac{1}{3}]}^1(\mu_2, \mathbf{Z}/2\mathbf{Z})$. We show that $\text{Ext}_{\mathbf{Z}[\frac{1}{3}]}^1(\mu_2, \mathbf{Z}/2\mathbf{Z})$ is trivial. Let $K = \mathbf{Q}$, $p = 2$ and $S = \{3\}$. It suffices to show that the homomorphism

$$(3) \quad \mathbf{Z}[\frac{1}{6}]^*/\mathbf{Z}[\frac{1}{6}]^{*2} \longrightarrow \mathbf{Q}_2^*/\mathbf{Q}_2^{*2}$$

is injective. The non-squares in $\mathbf{Z}[\frac{1}{6}]^*$ are generated by 2, 3 and -1 . By Lemma 4.1, the non-squares in \mathbf{Q}_2^* are generated by 2, 3 and 5. Hence the homomorphism in (3) is injective.

The extension group $\text{Ext}_{\mathbf{Z}[\frac{1}{2}, i]}^1(\mu_3, \mathbf{Z}/3\mathbf{Z})$. Let $K = \mathbf{Q}(i)$, $p = 3$ and $S = \{(1+i)\}$. Hence $O_S = \mathbf{Z}[i, \frac{1}{2}]$. The group Γ is the Galois group of the extension $\mathbf{Q}(\zeta_{12})/\mathbf{Q}(i)$ and has order 4. The cyclotomic character ω at 3 is quadratic, so ω^2 is trivial. The Hilbert class field of $\mathbf{Q}(\zeta_{12})$ is trivial. We will show that the group $\text{Ext}_{\mathbf{Z}[\frac{1}{2}, i]}^1(\mu_3, \mathbf{Z}/3\mathbf{Z})$ is trivial. It suffices to show that

$$\left(\mathbf{Z}[\zeta_{12}, \frac{1}{6}]^*/\mathbf{Z}[\zeta_{12}, \frac{1}{6}]^{*3} \right)^\Gamma \longrightarrow (\mathbf{Q}_3(\zeta_{12})^*/\mathbf{Q}_3(\zeta_{12})^{*3})^\Gamma$$

is injective.

Let F_1 be the functor from the category of $\mathbf{Z}[G_{\mathbf{Q}}]$ -modules to the category of $\mathbf{Z}[\Gamma]$ -modules defined by taking $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\zeta_{12}))$ -invariants. The functor F_1 sends injective objects to acyclic ones. Similarly, let F_2 be the functor of taking Γ -invariants from the category of $\mathbf{Z}[\Gamma]$ -modules to the category of abelian groups. We apply Theorem 2.1 with the two functors F_1 and F_2 described above, and we take the object A of Theorem 2.1 to be the $G_{\mathbf{Q}(i)}$ -module μ_3 . Since the order of Γ is coprime with the order of μ_3 , the derived functors of F_2 are zero. From the long exact sequence of Theorem 2.1 we see that

$$\left(\mathbf{Z}[\zeta_{12}, \frac{1}{6}]^*/\mathbf{Z}[\zeta_{12}, \frac{1}{6}]^{*3} \right)^\Gamma \simeq \mathbf{Z}[\frac{1}{6}]^*/\mathbf{Z}[\frac{1}{6}]^{*3}$$

and that

$$(\mathbf{Q}_3(\zeta_{12})^*/\mathbf{Q}_3(\zeta_{12})^{*3})^\Gamma \simeq \mathbf{Q}_3^*/\mathbf{Q}_3^{*3}.$$

We proceed as in the previous example.

The extension group $\text{Ext}_{\mathbf{Z}[\frac{1}{7}]}^1(\mu_2, \mathbf{Z}/2\mathbf{Z})$. Let $K = \mathbf{Q}$, $p = 2$ and $S = \{7\}$. Note that -7 is a 2-adic square. Hence the kernel of

$$\mathbf{Z}[\frac{1}{14}]^*/\mathbf{Z}[\frac{1}{14}]^{*2} \longrightarrow \mathbf{Q}_2^*/\mathbf{Q}_2^{*2}$$

is non-trivial and of order 2. A non-trivial extension of μ_2 by $\mathbf{Z}/2\mathbf{Z}$ over $\mathbf{Z}[\frac{1}{7}]$ is generically isomorphic to the extension $T(-7)$ of $\mathbf{Z}/2\mathbf{Z}$ by μ_2 . However, this extension is locally at 2 a trivial extension. The Hopf algebra of such a non-trivial extension is given by

$$\mathbf{Z}[\frac{1}{7}][X, Y]/(X^2 - X - Y, Y^2 + 2Y)$$

with coalgebra maps Δ (comultiplication), ϵ (counit) and S (coinverse):

$$\Delta(X) = X \otimes 1 + 1 \otimes X - 2X \otimes X + \frac{1}{7}Y \otimes Y - \frac{2}{7}(Y \otimes XY + XY \otimes Y) + \frac{4}{7}(XY \otimes XY)$$

$$\Delta(Y) = Y \otimes 1 + 1 \otimes Y + Y \otimes Y$$

$$\epsilon(X) = 0, \quad \epsilon(Y) = 0$$

$$S(X) = -X, \quad S(Y) = Y.$$

This group scheme is isomorphic to the 2-torsion subgroup scheme of the elliptic curve $J_0(49)$.

REFERENCES

- [KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.
- [Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.
- [Sch03] René Schoof. Abelian varieties over cyclotomic fields with good reduction everywhere. *Math. Ann.*, 325(3):413–448, 2003.
- [Sch09] René Schoof. Semistable abelian varieties with good reduction outside 15, 2009. preprint.
- [Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.